Шифр Ришилье

Шифр Ришелье (Франция, XVII-XVIII вв.) относится к шифрам перестановки. Ключом к шифру являются различные перестановки. Например: (4213)(51243)(132)(1432). Длина сообщения и количество цифр ключа должны совпадать.

Для шифрования ключ подписывается под сообщением, сообщение разбивается на части, соответствующие перестановкам и в каждой части производится своя перестановка букв.

Например, для сообщения УНИВЕРСИТЕТМИРЭА и ключа (4213)(51243)(132)(1432) шифрование будет выглядеть следующим образом:

Таблица 18. Пример шифрования

Исходное сообщение	(УНИВ)(ЕРСИТ)(ЕТМ)(ИРЭА)
Ключ	(4213)(51243)(132)(1432)
Зашифрованное сообщение	внуитерисемтиаэр

Для расшифрования метод аналогичен, а ключ меняется – для каждой перестановки исходного ключа находятся обратные перестановки, составляющие ключ расшифрования. Например, для ключа (4213)(51243)(132)(1432) обратным будет ключ (3241)(23541)(132)(1432), потому что суперпозиция этих ключей дает тождественную перестановку.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	ватсярианве
Ключ	(2143)(312)(4312)

Вариант 2

Зашифрованное сообщение	гбанаешлдд__каак
Ключ	(4123)(24513)(312)(2143)

Вариант 3

Зашифрованное сообщение	_виг янк_е оан икр_
Ключ	(1342)(31542)(132)(3124)

Вариант 4

Зашифрованное сообщение	анди япок_нге неаг
Ключ	(2314)(15432)(231)(4312)

Вариант 5

Зашифрованное сообщение	мьла авта_ лле т_та
Ключ	(1432)(24153)(213)(2413)

Вариант 6

Зашифрованное сообщение	лиАжКр_ира
Ключ	(2413)(312)(231)

Вариант 7

Зашифрованное сообщение	бикерентаик
Ключ	(321)(4213)(1423)

Вариант 8

Зашифрованное сообщение	инистиктутсувстсноенг теоинлатлке
Ключ	(52134)(461235)(15243)(34125)(45123)(265143)

Вариант 9

Зашифрованное сообщение	ПСПОРТКВЕРДНЕАОСКОГ
Ключ	(54132)(3241)(25314)(312)(21)

Вариант 10

Зашифрованное сообщение	ЦУИЛСАРТЫМОНАК
Ключ	(4132)(2143)(321)(132)

Азбука Морзе

Азбука Морзе – азбука, в которой буквы закодированы с помощью кода Морзе. Изначально использовалось название «Код Морзе», но с началом Первой мировой войны выросла необходимость передачи буквенных кодов, код стал называться азбукой. В разной справочной литературе можно встретить разный «набор» азбуки: с включением только букв или с включением также цифр и знаков препинания. Наравне с названиями «Код Морзе» и «Азбука Морзе» популярно также название «Морзянка». С учетом тематики нашего сайта детально будет показан только русский алфавит Морзе.

Код Морзе изобретен в 1838 году, назван в честь его создателя Сэмюэля Морзе. Первая депеша по способу Морзе была послана между Вашингтоном и Балтимором 24 мая 1844 года с текстом «Вот что творит Бог».

Код задает способ кодирования знаков последовательностью звуковых сигналов по определенным правилам. Код позволяет кодировать цифры, буквы, знаки пунктуации, служебные символы посредством длинных сигналов (тире) и коротких (точек). Сэмюэлю Морзе принадлежит идея кодирования, который приписывал себе изобретение телеграфа. Кодирование букв, а возможно и цифр, осуществил Альфред Вейлор (коллега Морзе). Позже код усовершенствовал Фридрих Герке. Под международным телеграфным кодом, включающим 26 латинских букв, 10 цифр, знаки препинания и служебные символы, также понимается код Морзе.

Особенностью кода Морзе является то, что точки и тире имеют разную длительность, что позволяет различать их на слух. Кроме того, код Морзе использует паузы между сигналами для разделения букв и слов.

Таблица 19. Азбука Морзе

Буква/ Символ	Код Морзе	Буква/ Символ	Код Морзе	Буква/ Символ	Код Морзе
А	.-	Б	-...	В	.--
Г	--.	Д	-..	Е	.
Ж	...-	З	--..	И	..

Окончание табл. 19

Буква/ Символ	Код Морзе	Буква/ Символ	Код Морзе	Буква/ Символ	Код Морзе
Й	.---	К	-.-	Л	.-..
М	--	Н	-.	О	---
П	.--.	Р	.-.	С	...
Т	-	У	..-	Ф	..-.
Х	....	Ц	-.-.	Ч	---.
Ш	----	Щ	--.-	Ъ	--.--
Ы	-.--	Ь	-..-	Э	..-..
Ю	..--	Я	.-.-	.	.-.-.-
,	--..--	-	-....-	!	-.-.--

Таблица 20. Пример шифрования

Сообщение	М	И	Р	Э	А
Зашифрованное сообщение	--	..	.-.	..-..	.-

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	... . .-. -.-- . / --. .-.. .- --.. .- / -....- / .-. .- ... .-- . - --..-- / .--. .- .-. --- .... --- -.. -. .- .-.- / ... .. .-. . -. .- --..-- / -.. --- ...- -.. -..- --..-- / .-. .- --.. .-.. ..- -.- .- --..-- / ... . .-. -.-- .--- / ... .-.. . -.. / -.. .- / .-- .. -. - --- -- / -... . --. ..- --.- . .--- / .--. . -. -.-- .-.-.-

Вариант 2

Зашифрованное сообщение	.--. .-. . -.. .-- .. ...- ..- / .-- ... # ---... / .-- .- ... / --- ... -.- --- .-. -... .. - / .--. . ---. .- .-.. -..- -. --- .--- / - .- .--- -. -.-- / --- -... --.-- .-.- ... -. . -. -..- . .-.-.- / -.- .- -.- --- . / --. --- .-. -..- -.- --- . / .--. .-. . --.. .-. . -. -..- . / .-- .- ---- / --. --- .-. -.. -.-- .--- / .-- --.. --. .-.. .-.- -.. / .. --.. --- -... .-. .- --.. .. - -.-.--

Вариант 3

Зашифрованное сообщение	.--. .-. . -.. .-- .. ...- ..- / .-- ... . ---... / .-- .- ... / --- ... -.- --- .-. -... .. - / .--. . ---. .- .-.. -..- -. --- .--- / - .- .--- -. -.-- / --- -... --.--.-.- ... -. . -. -..- . .-.-.- / -.- .- -.- --- . / --. --- .-. -..- -.- --- . / .--. .-. . --.. .-. . -. -..- . / .-- .- ---- / --. --- .-. -.. -.-- .--- / .-- --.. --. .-.. .-.- -.. / .. --.. --- -... .-. .- --.. .. - -.-.--

Вариант 4

Зашифрованное сообщение	. ... - -..- / ...- . -. --.- .. -. -.-- / .-- / .-. ..- ... ... -.- .. .... / ... . .-.. . -. -..- .-.- .... / ... / ... .--. --- -.- --- .--- -. --- ..-- / .-- .- ...- -. --- ... - -..- ..-- / .-.. .. -.-. --..-- / ... / -.- .-. .- ... .. .-- --- ..-- / ... .. .-.. --- .--- / .-- / -.. .-- .. ...- . -. -..- .-.- .... --..-- / ... / .--. --- .... --- -.. -.- --- .--- --..-- / ... --- / .-- --.. --. .-.. .-.- -.. --- -- / -.-. .-.-. .. -.-.

Вариант 5

Зашифрованное сообщение	- -.-- / .... --- .-. --- ---- .- .-.- / --- ---. . -. -..- / -....- / --.. -. .- ..- - .-.-.- / .-.- / - . -... . / -. .. -.- --- --. -.. .- / -. . / .-.. --. ..- .-.-.- / .--. --- ---. . -- ..- -....- - --- / - --- .-.. -..- -.- --- / ... -.- .-. -.-- .- - .- ..-- --..-- / ---. - --- / .-.. ..-- -... .. - -..- / - . -... .-.- / -. . / ----- --. ..-

Вариант 6

Зашифрованное сообщение	..- / .-.. ..- -.- --- -- --- .-. -..- .-.- / -.. ..- -... / --.. . .-.. . -. -.-- .--- --..-- / --.. .-.. .- - .- .-.- / -.-. . .--. -..- / -. .- / -.. ..- -... . / - ---- -- --..-- / .. / -.. -. . -- / .. / -. --- ---. -..- ..-- / -.- --- - / ..- ---. . -. -.-- .--- / .-- ... . / .... --- -.. .. - / .--. --- / -.-. . .--. .. / -.- .-. ..--. --- -- .-.-.-

Вариант 7

Зашифрованное сообщение	-... . .-.. . . - / .--. .- .-. ..- ... / --- -.. .. -. --- -.- --- .--- / .-- / - ..--- .- -. . / -- --- .-. .-.- / --. --- .-.. ..- -... --- -- -.-.-- / ---. - --- / .. --.- . - / --- -. / .-- / ... - .-. .- -. . / -.. .- .-.. . -.- --- .--- ..--.. / -.--. - --- / -.- .. -. ..- .-.. / --- -. / .-- / -.- .-. .- ..-- / .-. --- -.. -. ---- ..--..

Вариант 8

Зашифрованное сообщение	.-- / ..-.. - --- - / .-.. . ... / --.. .- .-- --- .-. --- ...- . -. -. -.-- .--- --..-- / .--. --- / .--. ..- ---- .. -. -.- .- -- / ... . .-. . -... .-. .- --..-- / .-.- / ... / .-- .. -. - --- .-- -.- --- .--- / --.. .- .-. .-.- ...- . -. -. --- .--- / -. .- / --- .... --- - ..- / ---- . .-.. / .-- ---. . .-. .- .-.-.-

Вариант 9

Зашифрованное сообщение	--.. .- / --. --- .-. .- -- .. --..-- / --.. .- / .-.. . ... .- -- .. --..-- / --.. .- / ---- .. .-. --- -.- .. -- .. / -- --- .-. .-.- -- .. --..-- / -. . / -. .- / -. . - ... . / -....- / -. .- / --.. . -- .-.. . / ...- .. .-.. / ... - .- .-. .. -.- / .-- / --- -.. -. --- -- / ... . .-.. . .-.-.-

Вариант 10

Зашифрованное сообщение	.. / ... - .-. .- -. -. --- .--- / -... .-.. .. --.. --- ... - -..- ..-- / --.. .- -.- --- .-- .- -. -. -.-- .--- --..-- / ... -- --- - .-. ..-- / --.. .- / - . -- -. ..- ..-- / .-- ..- .- .-.. -..- --..-- / .. / .-- .. ...- ..- / -... . .-. . --. / --- --- . .- .-. --- .-- .- -. -. -.-- .--- / .. / --- ---. .- .-. --- .-- .- -. -. ..- ..- - / -.. .- .-.. -..- .-.-.-

Шифр Вернама

В 1917 году телеграфист Гильберт Вернаам изобрел шифр, основанный на побитном исключающем “ИЛИ”. Если говорить кратко и просто, то для каждой буквы исходного сообщения подбирается другая маскирующая буква, которая делает исходное сообщение нечитаемым.

Система симметричного шифрования, изобретённая в 1917 году Гилбертом Вернамом. Шифр является разновидностью криптосистемы одноразовых блокнотов. В нём используется булева функция «исключающее или». Шифр Вернама является примером системы с абсолютной криптографической стойкостью. При этом он считается одной из простейших криптосистем.

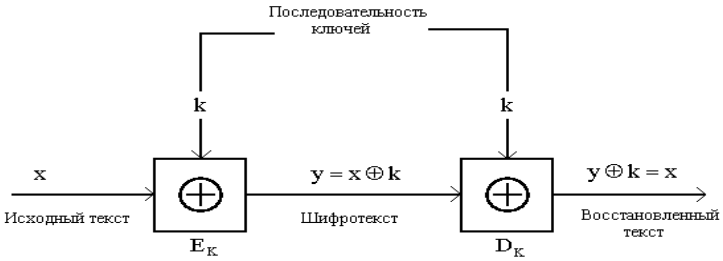

Рисунок 19. Криптосистема Вернама

Для получения шифротекста открытый текст объединяется операцией «исключающее или» с секретным ключом. Так, например, при применении ключа (1 1 1 0 1) на букву «Б» (0 0 0 0 1) получаем зашифрованное сообщение (11100): (00001) ⊕ (11101) = (11100) Зная, что для принимаемого сообщения имеем ключ (1 1 1 0 1), легко получить исходное сообщение той же операцией: (11100) ⊕ (11101) = (00001) Для абсолютной криптографической стойкости ключ должен обладать тремя критически важными свойствами[:

1) иметь случайное дискретное равномерное распределение: P k (k) = 1 / 2 N(степень) , где k — ключ, а N — количество бинарных символов в ключе;

2) совпадать по размеру с заданным открытым текстом;

3) применяться только один раз.

Таблица 21. Таблица истинности исключающее ИЛИ (⊕)

x	y	x⊕y
0	0	0
0	1	1
1	0	1
1	1	0

Для шифрования будет использоваться следующая таблица Кодов.

Таблица 22. Таблица кодов

№	Буква	Двоичный код	№	Буква	Двоичный код	№	Буква	Двоичный код
1	А	00000001	12	К	00001100	23	Х	00010111
2	Б	00000010	13	Л	00001101	24	Ц	00011000
3	В	00000011	14	М	00001110	25	Ч	00011001
4	Г	00000100	15	Н	00001111	26	Ш	00011010

Окончание табл. 22

№	Буква	Двоичный код	№	Буква	Двоичный код	№	Буква	Двоичный код
5	Д	00000101	16	О	00010000	27	Щ	00011011
6	Е	00000110	17	П	00010001	28	Ъ	00011100
7	Ё	00000111	18	Р	00010010	29	Ы	00011101
8	Ж	00001000	19	С	00010011	30	Ь	00011110
9	З	00001001	20	Т	00010100	31	Э	00011111
10	И	00001010	21	У	00010101	32	Ю	00100000
11	Й	00001011	22	Ф	00010110	33	Я	00100001
0			00000000			. (точка)		

Пример
Исходное сообщение МИРЭА
Ключ АБВГД
Шифрование буквы М с ключом А:
00001110⊕00000001 = 00001111 (Н)
Шифрование буквы И с ключом Б:
00001010⊕ 00000010= 00001000 (Ж)
Шифрование буквы Р с ключом В:
00010010⊕ 00000011= 00010001 (П)
Шифрование буквы Э с ключом Г:
00011111⊕ 00000100= 00011011 (Щ)
Шифрование буквы А с ключом Д:
00000001⊕ 00000101= 00000100 (Г)

Таблица 23. Пример шифрования

Исходное сообщение	МИРЭА
Ключ	АБВГД
Зашифрованное сообщение	НЖПЩГ

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	рв.йввэ
Ключ	абрикос

Вариант 2

Зашифрованное сообщение	опх.кфл
Ключ	садовод

Вариант 3

Зашифрованное сообщение	мяо.ыещ
Ключ	варенье

Вариант 4

Зашифрованное сообщение	цтщмглр
Ключ	черника

Вариант 5

Зашифрованное сообщение	бчдэждб
Ключ	пломбир

Вариант 6

Зашифрованное сообщение	б.ыысу
Ключ	компот

Вариант 7

Зашифрованное сообщение	эюлт.э
Ключ	лагуна

Вариант 8

Зашифрованное сообщение	.йаурьб
Ключ	система

Вариант 9

Зашифрованное сообщение	э.чп.
Ключ	питон

Вариант 10

Зашифрованное сообщение	шёцэыдмъм
Ключ	чебурашка

Шифр ADFGVX

В 1918 году во время первой мировой войны в Германии была применена шифровальная система ADFGVX. Этот шифр был введен в употребление Фрицем Небелем, офицером связи, служившим в штабе германской армии. Свое название эта система получила из-за того, что ее шифрограммы содержали только буквы A, D, F, G и X. Впоследствии была добавлена буква V, и шифр стал называться шифром ADFGVX.

Процесс шифрования начинается с создания сетки размером 6x6, каждая ячейка которой содержит 26 букв и 10 цифр. Каждая строка и столбец этой сетки обозначаются одной из 6 букв - “A”, “D”, “F”, “G”, “V” и “X”. Эти буквы используются для обозначения столбцов и строк, что делает процесс дешифровки сложным, поскольку получателю нужно знать точное расположение каждой ячейки, чтобы правильно расшифровать сообщение.

Пример

Сообщение: UNIVERSITY

Таблица 24. Сетка для шифрования

	A	D	F	G	V	X
A	1	J	R	4	H	D
D	E	2	A	V	9	M
F	8	P	I	N	K	Z
G	B	Y	U	F	6	T
V	5	G	X	S	3	O
X	W	L	Q	7	C	0

Шаг 1. Замена. Каждый символ сообщения заменяется на пару букв, обозначающих строку и столбец соответствующего символа в сетке.

Таблица 25. Шаг 1

Сообщение	U	N	I	V	E	R	S	I	T	Y
Шифротекст после замены	GF	FG	FF	DG	DA	AF	VG	FF	GX	GD

Шаг 2. Перестановка. Создаётся новая таблица с ключевым словом в верхней строке. В качестве ключа в данном примере слово «DRIVE». Обычно используются более длинные ключевые слова или фразы.

Таблица 26. Шаг 2

D	R	I	V	E
G	F	F	G	F
F	D	G	D	A
A	F	V	G	F
F	G	X	G	D

Шаг 3. Далее буквы ключевого слова переставляются в алфавитном порядке вместе с соответствующими им столбцами сетки.

Таблица 27. Шаг 3

D	E	I	R	V
G	F	F	F	G
F	A	G	D	D
A	F	V	F	G
F	D	X	G	G

После чего столбцы по очереди записываются в одну строку, образуя зашифрованный текст.

Окончательный вид шифротекста: GFAFFAFDFGVXFDFGGDGG

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	AFDFVFDAXVFA
Ключ	kib

Вариант 2

Зашифрованное сообщение	FADXVDXGVFFVXFAAADGF
Ключ	round

Вариант 3

Зашифрованное сообщение	AFDXVGDXXFFXAGVGFF
Ключ	sun

Вариант 4

Зашифрованное сообщение	DVFFFFGXXDFGAADVGGXF
Ключ	group

Вариант 5

Зашифрованное сообщение	DGFXFXGAAGFVDXADFXFV
Ключ	lecture

Вариант 6

Зашифрованное сообщение	DVAXFVDFAA
Ключ	kib

Вариант 7

Зашифрованное сообщение	GAVFVDGDFAVAADADDFAGFA
Ключ	key

Вариант 8

Зашифрованное сообщение	FFDDXAVXFGFA
Ключ	moon

Вариант 9

Зашифрованное сообщение	GDDDDFFXGAFFDF
Ключ	poem

Вариант 10

Зашифрованное сообщение	DFDFAXXFGD
Ключ	note

Шифр Хилла

Шифр Хилла — некий шифр подстановки, который в 1929 году разработал математик Лестер С. Хилл. Данный шифр основывается на линейной алгебре.

Шифрование

Открытый текст представляет собой n-мерный вектор. Ключ – квадратная матрица размера n x n. Для получения шифротекста ключ умножается на открытый текст по модулю выбранной числовой схемы, в случае русского алфавита - 33.

Пусть "$p_1p_2p_3$" – открытый текст, ключ – матрица размера 3 x 3 и шифротекст – вектор размерности – 3, "$c_1c_2c_3$" соответственно.

В общем виде: C = K*P

В матричном виде эта система описывается так: